Steganographic Data Injection by Angle Dependent Variable Amplitude Diminution for Enhanced Security in RFID Chips

19 May 2025
Simon Edwards
Research Acceleration Initiative

Introduction

Although RFID banking chips are certainly more secure than the legacy magnetic swipe method, it would be ideal if there were a method for differentiating between a spoofed chip transmitting an authentic, encrypted card number through a seemingly legitimate point of sale device.

Point of sale devices capable of relaying credit card information through the SWIFT network are relatively easy to obtain and can easily be abused. Any security features built into either the point of sale device or the transmitted data from the RFID chip, itself, could easily be identified by sophisticated adversaries. However, with the proper implementation, it should be possible to create a system of verification of the authenticity of a chip which would likely be difficult to identify, even under the scrutiny of a reverse engineer.

Abstract

In order for the following method to work, it would be necessary for raw data concerning amplitude of return signal (which could be megabytes per transaction) to be transmitted to a secure server in addition to the basic information which identifies the chip being used. The server would then have to analyze the raw data in order to find a hidden pattern which could not be identified except by someone who knew for what to seek. This proposal would create an increased demand for processing power on the end of payment processor as well as increase bandwidth needs, but would afford an opportunity to identify fraud which relies upon the secrecy of the methods involved, much for the same reason that anti-counterfeiting measures work best when they are kept secret.

In addition to employing traditional capacitors within the RFID chip, the material from which the chip is composed could be designed to partially block the emitted signal from the antennae to a different degree depending upon the angle at which the card is held relative to the reader and whereas the entire substrate may be asymmetrically charged, electrically. An authentic chip with this security feature would emit radio frequency at a variable amplitude, therefore, depending upon the angle at which the chip is oriented relative to the reader in addition to varying with distance. Depending upon how the chip is "charged," the amplitude output characteristics would also vary, with multiple, disparate codes being broadcast from different parts of the chip simultaneously at different frequencies and with the introduction of "chaff" by the point of sale machine, whether it has or has not been programmed to emit chaff. With the introduction of chaff, a simple modifier may be applied to the logic of the chip itself which is dictated by the payment processor. The purpose of the chaff is to prevent a reverse engineer from comprehensively understanding or being able to predict the appropriate

behavior of the chip through experimentation. In the absence of a legitimate modifier, a transaction could be blocked or flagged as suspicious (this concept was first promulgated in 7 May 2024.) In most cases, it is better to permit the fraudulent transaction for investigatory purposes and to later reimburse the customer so that the defrauder does not discover the security feature and does not become aware of the discovery of the fraud.

Although one might look for any fluctuation in amplitude parameters as a “liveness test” to establish that a human being is holding the card, this method has as its advantage, furthermore, that more subtle and abrupt changes to amplitude may be manifest which could not be the result of a hand tremor, for example, but which are connected to rotational re-orientation of the chip and which involve abrupt drop-offs in amplitude which, although subtle, are not gradual in the temporal respect.

As this security feature would be rooted not in a logical function, but in the physical structuring of the chip’s capacitance substrate (via the introduction of variable thickness, foreign metallic compounds with different properties of capacitance and RF insulators in specific combinations) there would be no straightforward way of mimicking the behavior of an authentic chip as, to do so, one would have to also duplicate the process of manufacture of the chip, which would be a closely guarded secret in any case. Even after someone became aware of this methodology, the attacker would have to test the behavior of the chip under an extremely large number of conditions as every single atom of the capacitance substrate would be capable of introducing a unique change to the overall behavior of the system. In computer science, the best analog to this kind of attack would be attacks based upon what are known as rainbow tables. Rainbow tables become impractical when the number of potential combinations grows too cumbersome. Ideally, within this system, every atom within the capacitance substrate would introduce a unique element of a dynamic which affects the overall performance of the system which would be so unique that one would need to know precisely how a specific chip was manufactured in order for appropriate emission behavior to be mimicked. By requiring the broadcast of large volumes of analog data unique to specific combinations of angular orientation and position relative to the RF power source, it becomes far more difficult for an adversary to bruteforce to find acceptable patterns of output. Importantly, the method does not require the redesign of POS terminals.

Conclusion

This security feature might best be used to support fraud investigations rather than to deny specific fraudulent transactions. Fraudulent transactions can always be rolled back at a later date in order to protect information concerning the nature of the fraud discovery.